5. The method according to claim 4, wherein the group-specific signature key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization.

6. The method according to claim 4, wherein the steps of assigning the group-specific signature key and the group-specific signature of the device-specific certificate to an associated specific group are each determined by comparing each key device with a stored list of approved key devices.

7. The method according to claim 4, further comprising the steps of:

establishing a link between at least two key devices;

transmitting a corresponding device-specific certificate and a corresponding device-specific signature key from one of the key devices to another one of the key devices, the another one of the key devices verifying authenticity of the corresponding device-specific certificate using the corresponding device-specific signature key according to the relationship:

$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD) = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a signature key of an administrator, sAD represents a secret key of the administrator, and Z(A) represents the corresponding device-specific certificate.

IN THE ABSTRACT:

Delete original page 7 and replace the Abstract with Replacement Page 7, which is provided on a separate sheet attached to the amendment.